Domestic Security Committee

Wednesday, February 22, 2006
1:00 P.M.
12 HOB

Action Packet

Allan G. Bense
Speaker

Sandra "Sandy" Adams
Chair

COMMITTEE MEETING REPORT

Domestic Security Committee

2/22/2006 1:00:00PM

Location: 12 HOB

Attendance:

	Present	*Absent*	*Excused*
Sandra Adams (Chair)	X		
Mary Brandenburg	X		
Dan Gelber	X		
Gayle Harrell	X		
Carlos Lopez-Cantera	X		
Dave Murzin	X		
Ari Porth	X		
Everett Rice	X		
Priscilla Taylor	X		
Totals:	**9**	**0**	**0**

Committee meeting was reported out: Wednesday, February 22, 2006 5:05:49PM

COMMITTEE MEETING REPORT

Domestic Security Committee

2/22/2006 1:00:00PM

Location: 12 HOB

Other Business Appearance:

Disaster Preparedness and Response
Eve Rainey, Bureau Chief (Lobbyist) (State Employee) - Information Only
DCA/DEM
2555 Shumard Oak Blvd.
Tallahassee Florida 32399
Phone: 850-413-9914

Disaster Preparedness and Response
David Mica, Executive Director (Lobbyist) (At Request Of Chair) - Information Only
Florida Petroleum Council
215 S. Monroe St.
Tallahassee Florida 32301
Phone: 561-6300

Disaster Preparedness and Response
Linda Canton, Director (General Public) - Information Only
No Person Left Behind
704 Homer Ave. North
Lehigh Acres Florida 33971
Phone: 239-368-6846

Disaster Preparedness and Response
Jim Smith, President/CEO (Lobbyist) - Information Only
Florida Petroleum Marketers and Convenience Store Assoc.
209 Office Plaza Dr.
Tallahassee Florida 32301
Phone: 850-877-5178

Disaster Preparedness and Response
Linda Carter, Director (General Public) - Information Only
No Person Left Behind
704 Homer Ave. North
Lehigh Acres Florida 33971
Phone: 239-368-6846

Seaport Security
Michael Rubin, Vice President (Lobbyist) - Information Only
Florida Ports Council
502 E. Jefferson St.
Tallahassee Florida 32303
Phone: 850-222-8028

Seaport Security
Chuck Towsley, Port Director (General Public) - Information Only
Port of Miami-Dade
1015 N. America Way
Miami Florida 33132
Phone: 305-347-4844

COMMITTEE MEETING REPORT

Domestic Security Committee

2/22/2006 1:00:00PM

Location: 12 HOB

Seaport Security
Richard A. Wainio, Tampa Port Director (General Public) - Information Only
Tampa Port Authority/Florida Port Council
1101 Channerside Dr.
Tampa Florida 33602
Phone: 813-905-5104

Seaport Security
Steve Vogt, Director of Public Safety (General Public) - Proponent
Port Canaveral
2000 George King Blvd.
Cape Canaveral Florida 32920
Phone: 321-783-7831

Seaport Security
Nevin Smith, Seaport Security Administrator (State Employee) - Information Only
Florida Department of Law Enforcement
Tallahassee Florida
Phone: 850-410-7067

Seaport Security
Kathy Andress, Deputy Port Director (General Public) - Information Only
Port or Palm Beach
One East 11th Street
Riveria Beach Florida 33404
Phone: 561-383-4151

Seaport Security
Phillip Allen, Director (General Public) - Information Only
Port Everglades
1850 Eller Dr.
Ft. Lauderadle Florida 3316-4201
Phone: 954-462-3516

Seaport Security
Andrew Benard, Chief, Counter Drug Law Enforcement (State Employee) - Proponent
Office of Drug Control
PL04, The Capitol
Tallahassee Florida 32399
Phone: 850-488-9557

Seaport Security
Charles N. White, Direcotr of Port Security (General Public) - Information Only
Port of Jacksonville
2831 Talleyard Ave.
Jacksonville Florida 32206-0005
Phone: 904-630-3055

Seaport Security
David McDonald, Exec. Director, Port of Manatee/Tamap Bay (General Public) - Information Only
Florida Ports Council
300 Tampa Bay Way
Palmetto Florida 34221
Phone: 941-722-6621

Committee meeting was reported out: Wednesday, February 22, 2006 5:05:49PM

COMMITTEE MEETING REPORT

Domestic Security Committee

2/22/2006 1:00:00PM

Location: 12 HOB

Seaport Security
Luis Mevricie, Business Agenct (General Public) - Information Only
International Longshoremen
1610 Pont Blvd.
Miami Florida 33132
Phone: 305-379-8695

Seaport Security
Eric Poole, Gov. Liaison (Lobbyist) - Information Only
Florida Assoc. of Counties
100 S. Monroe Street
Tallahassee Florida 32301
Phone: 922-4300

Committee meeting was reported out: Wednesday, February 22, 2006 5:05:49PM

COMMITTEE MEETING REPORT

Domestic Security Committee

2/22/2006 1:00:00PM

Location: 12 HOB

Summary: No Bills Considered

Committee meeting was reported out: Wednesday, February 22, 2006 5:05:49PM

[Code of Federal Regulations]
[Title 33, Volume 1]
[Revised as of July 1, 2003]
From the U.S. Government Printing Office via GPO Access
[CITE: 33CFR105.305]

[Page 367-369]

TITLE 33--NAVIGATION AND NAVIGABLE WATERS

CHAPTER I--COAST GUARD, DEPARTMENT OF HOMELAND SECURITY

PART 105--FACILITY SECURITY--Table of Contents

Subpart C--Facility Security Assessment (FSA)

Sec. 105.305 Facility Security Assessment (FSA) requirements.

(a) Background. The facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the facility, including:

(i) The location of each active and inactive access point to the facility;

(ii) The number, reliability, and security duties of facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel and visitors;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;

(4) Existing contracts with private security companies and existing agreements with local or municipal agencies;

(5) Procedures for controlling keys and other access prevention systems;

(6) Procedures for cargo and vessel stores operations;

(7) Response capability to security incidents;

(8) Threat assessments, including the purpose and methodology of the assessment, for the port in which the facility is located or at which passengers embark or disembark;

(9) Previous reports on security needs; and

(10) Any other existing security procedures and systems, equipment, communications, and facility personnel.

(b) On-scene survey. The facility owner or operator must ensure that an on-scene survey of each facility is conducted. The on-scene survey examines and evaluates existing facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) Analysis and recommendations. In conducting the FSA, the facility owner

[[Page 368]]

or operator must ensure that the FSO analyzes the facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey including but not limited to:

(i) Waterside and shore-side access to the facility and vessel berthing at the facility;

(ii) Structural integrity of the piers, facilities, and associated structures;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to services and utilities;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Adjacent areas that may be exploited during or for an attack;

(vii) Areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the facility;

(viii) Existing agreements with private security companies providing waterside and shore-side security services;

(ix) Any conflicting policies between safety and security measures and procedures;

(x) Any conflicting facility operations and security duty assignments;

(xi) Any enforcement and personnel constraints;

(xii) Any deficiencies identified during daily operations or training and drills; and

(xiii) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits;

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the facility or of a vessel moored at the facility;

(ii) Hijacking or seizure of a vessel moored at the facility or of persons on board;

(iii) Tampering with cargo, essential equipment or systems, or stores of a vessel moored at the facility;

(iv) Unauthorized access or use including the presence of stowaways;

(v) Smuggling dangerous substances and devices to the facility;

(vi) Use of a vessel moored at the facility to carry those intending to cause a security incident and their equipment;

(vii) Use of a vessel moored at the facility as a weapon or as a means to cause damage or destruction;

(viii) Blockage of entrances, locks, and approaches; and

(ix) Nuclear, biological, radiological, explosive, and chemical attack;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the facility's infrastructure, policies and procedures;

(5) Any particular aspects of the facility, including the vessels using the facility, which make it likely to be the target of an attack;

(6) Likely consequences in terms of loss of life, damage to property, and economic disruption, including disruption to transportation systems, of an attack on or at the facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) FSA report. (1) The facility owner or operator must ensure that a written FSA report is prepared and included as part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability;

(v) A list of the key facility operations that are important to protect; and

[[Page 369]]

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility.

(2) A FSA report must describe the following elements within the facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks;

(vi) Relevant transportation infrastructure; and

(vii) Utilities.

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
A. Access Control: Physical and Personnel Security		Access control is essential to seaport security. Easy access to port facilities, vessels and cargo holding areas facilitates internal conspiracies. Controlled access, especially to restricted cargo storage areas, is basic to deterring these conspiracies. Access control should conform to the following minimum standards:	
	1. ID Badges	a. All personnel permanently employed at the seaport (to include port management staff, tenant activity staff, truckers, stevedores, and longshoreman, etc.) will be required to display a picture ID badge or card at all times when accessing or working within restricted areas, as designated by port management. At a minimum, however, the following should be regarded as restricted areas: ▪ Cargo Storage or staging yards ▪ Docks/berths ▪ Fuel storage or transfer yards ▪ Cruise terminals This requirement also applies to day workers and casual labor who work at the port any more frequently than 5 days in any given 90-day period.	
		b. Picture ID's should be color coded or clearly identified by other means (e.g. hologram or symbol) to indicate areas to which access is authorized (e.g. Docks, cargo yards, marine terminals, administration buildings, or unrestricted access).	
		c. ID cards will be laminated and issued by serial number. Lost or stolen cards must be reported and a log maintained of all currently issued and rescinded cards.	
		d. Issuance of the Picture ID card (by Port Management) will be contingent on the successful completion of a fingerprint-based Criminal History Background Check. Personnel with felony convictions for serious and/or violent crimes during the previous 5 years (e.g. violent crimes against persons; delivery or trafficking of controlled substances, illegal narcotics or dangerous drugs; smuggling or theft, racketeering, fraud) should not be approved for issuance of an ID card.	
		e. Port Management must determine local procedures for permitting access by transient laborers or itinerant visitors and business people. At a minimum, these procedures will include logging in all personnel to whom a Port I.D. card has not been issued and issuance of a temporary or visitors pass.	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		f. I.D. cards will be renewed on an annual basis. Any felony conviction for the crimes noted above during the previous year will constitute grounds for denial or disapproval.	
	2. Personnel Security	a. Prospective employees will be required to provide background information about previous employment history, criminal records, and drug use.	
		b. Prospective employees will also be fingerprinted as part of the application process.	
	3. Visitor Access	a. Access to the seaport should require checking and recording the visitor's name, purpose of visit, destination, vehicle tag number, and date and time of entry/departure.	
		b. Visitors should be authorized access only to areas specific to their port business. Passes should be used to convey this permit.	
		c. Visitor vehicles should not be allowed on the dock or in restricted cargo areas.	
		d. Visitor vehicles must park only in designated areas.	
	4. Access Gates & Gate Houses	a. Gates and gate houses should control access to restricted areas as determined by port management. Gates should be located at all perimeter access points and principal interior access points. Gates and gate houses should conform to these standards:	
		b. Gates should be the minimum number to provide adequate access.	
		c. Gates/gate houses should be staffed or locked at all times	
		d. The construction of the gates should at least match the construction of the perimeter or interior fencing in general. (e.g. Be 8 feet high, nine (9) gauge galvanized steel, of two (2) inch wide chain link construction topped with an additional 2 foot barbed wire outrigger [outrigger consists of three strands of nine (9) gauge galvanized steel barbed wire] at forty five (45) degrees outward angle above the fence.)	
		e. Gate houses at all vehicle entrances and exits should be staffed during business hours unless controlled by electronic access systems. Gatehouses should be situated so that exiting vehicles may be halted and examined on seaport property.	
		f. Gate House personnel should be equipped with telephones or other communications devices.	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		g. Gate House personnel should be thoroughly trained in the procedures for processing and/or logging vehicular entry/exit.	
	5. Designated Parking	a. Parking is an important aspect of seaport security in general, and access control in particular. Parking within the seaport should be severely restricted, and should be authorized by a strictly enforced gate pass and/or decal system.	
		b. Passes or decals should be color or otherwise coded to further restrict access to authorized times and locations.	
		c. Parking for employees, dock-workers and visitors should be restricted to designated areas, off dock and outside of fenced operational, cargo handling and storage areas.	
		d. Parking for vehicles authorized on port grounds should be restricted largely to port authority, carrier, maintenance, commercial and government vehicles which are essential within the seaport or marine terminal. Parking for these vehicles should be restricted to fenced or clearly marked designated parking areas within the perimeter of the port.	
		e. Temporary permits or passes should be issued to vendors and visitors for parking in designated controlled areas.	
	6. Fencing	a. In general, fencing should establish a secure perimeter with controlled access. Where fencing is required (perimeter or interior), it should conform to these standards:	
		b. Be 8 feet high, nine (9) gauge galvanized steel, of two (2) inch wide chain link construction topped with an additional 2 foot barbed wire outrigger [outrigger consists of three strands of nine (9) gauge galvanized steel barbed wire] at forty five (45) degrees outward angle above the fence.	
		c. Bottom of fencing should be no more than two (2) inches from hard surface of concrete or asphalt. This surface should be sufficiently thick to prevent access from underneath.	
		d. The exterior and interior sides of the fence should be cleared and uncluttered by not less than five (5) feet to ensure that the integrity of the fence is not compromised (i.e., no containers or other objects against fence.)	
			Enhancement for construction of new fencing: Reinforcement of the fence line with a barrier (e.g., ditch or berm) is recommended to enclose wheeled operations

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
			involving containers on chassis or trucks loaded with consolidated cargoes overnight, to render certain parts of the fence line physically impassible for a truck or trailer.
	7. Lighting	a. In general, lighting should be sufficient to adequately illuminate port operations and cargo areas. As a rule, port facilities should be illuminated at least to the level of twilight. Lighting must conform to federal regulations, and should comply with voluntary agreements such as the U.S. Customs Sea Carrier or Super Carrier Initiatives. Further, lighting should conform to these standards:	
		b. It must not interfere with safe vessel navigation (33CFR 154.570 (d))	
		c. Lighting must be provided sunset to sunrise. (OSHA 2232 1917.123)	
		d. Lighting should be high-mast, sufficient for adequately illuminating exterior gates, piers, cargo areas, cargo traffic areas and all working and walking areas	
		e. Lights should be properly spaced	
		f. Updated lighting technology should be used, such as: high pressure sodium, mercury vapor, or metal halide lighting.	
		g. Lighting should be directed downward, away from guards or offices, and should produce high contrasts with few shadows.	
		h. Dock work areas, including container unloading and loading areas, should have five (5) foot candle illumination.	
		i. Container/cargo yards should have, at least, 1 foot-candle illumination. Dark or blind spots should not exist.	
		j. If security vehicles are used, they should be equipped with spotlights that enable security personnel to look down through rows of containers.	
	8. Use of Signs	a. Signs are inexpensive deterrents and should be strategically posted throughout the port and where ever access is restricted to authorized personnel.	
		b. A sign conveying Customs authority and stating something similar to "This Port Is A Border Entry Point and All Persons, Effects, and Vehicles Are Subject to Search Under Federal Statute 19 United States Code Sec 981 (f)" should be posted at main exterior access points, vessel gangways and all restricted areas. Signs should conform to these minimum standards:	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		c. Be highly visible with high contrast background and lettering; signs should be visible at night illuminated by lights or iridescent lettering.	
		d. Be of sufficient size and boldness	
		e. Bilingual signs should be considered, if appropriate	
	9. Locks and Keys	a. Key control should be implemented to delineate which personnel have right of access to specified areas. Key control should include a master ledger recording the legitimate holder of each copy of each key, issuance for which should be controlled by management or security personnel.	
		b. Locks, locking devices, and key control systems should be inspected regularly, and malfunctioning equipment repaired or replaced.	
		c. Keys will be removed and secured from cargo handling equipment and vehicles when not in use.	
		d. Only case hardened locks and chains will be used, with chains permanently attached to fence posts/gates.	
	10. Maintenance of Infrastructure	An adequate maintenance system, comprised of regularly scheduled inspections to keep fencing, gates, lighting and cameras in good condition and working order should be implemented.	
Access Control Enhancements			
	11. Intrusion Detection Systems		Intrusion Detection Systems, including video monitoring, remote sensors and alarms, and computerized recording instrumentation, may be employed to facilitate real-time evaluation and response and subsequent investigation and analysis.
	12. Closed Circuit Television (CCTV)		a. Closed Circuit Television Cameras are recommended and should be used when warranted by security threat. Cameras should be placed at main entrances and exits and in areas with high risk and/or high value

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
			cargo. Cameras should:
			b. Be able to record at relatively low levels of light.
			c. Have remote control and zoom lens capacity (at least 8X) when used for surveillance.
			d. Be capable of being monitored at same time.
			e. Have video tape record capabilities
			f. Be equipped with a recording mechanism to video record vehicles and persons entering and exiting the facility. (This also acts as a deterrent, especially when used in conjunction with signage.)
			g. Cameras could be used at gates for simultaneously recording I.D/photo and personnel.
B. Operational and Procedural Security		Operational and Procedural Security is integral to seaport security. Through development and enforcement of policies and procedures, port management sends a clear message that security is taken seriously at this port.	
	1. Standing Security Committee	Port Management will sponsor/conduct a regularly scheduled forum (not less than once per quarter) at which all stakeholders in port security are invited to participate and to discuss security issues.	
	2. Security Master Plan	Port Management will include security related initiatives in the port's strategic or master plan. These initiatives should identify and prioritize projected capital outlays for security-related projects.	
	3. Standard Operating Procedures (SOPs)	a. Port Management shall provide a current security manual incorporating standard operating procedures (SOPs), standards of conduct & responsibilities of appropriate security and management personnel, and a definitive statement of what management expects of its security force personnel.	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		b. The Port Security Director should formulate written operating procedures for security-related matters, including bomb threats and alert levels, and should collaborate with relevant government and law enforcement agencies to develop an emergency response plan.	
		c. Managers must review procedures periodically to ensure that new threats and procedural vulnerabilities are identified as they arise.	
	4. Law Enforcement Presence	Port Management will take steps necessary (e.g. through contracting or other means) to ensure the routine, scheduled presence at the port of security patrols by sworn law enforcement personnel.	Where feasible, management should work with local authorities to negotiate for the permanent assignment to the port of a dedicated, full time unit of sworn, law enforcement personnel.
	5. Security Guards	a. Guard Service is a critical human component of a security system. Great care must be used in selecting a guard service, and/or security personnel. The primary criteria for selecting guard service or security personnel should not be least or even low cost. Equally important, care should be taken in training and maintaining qualified personnel. At a minimum, guards or security personnel should:	
		b. Wear uniforms that are complete, distinct, and authoritative.	
		c. Have 2-way radios with capability to promptly reach back-up support.	
		d. Provide adequate patrols to include roving security, building, perimeter and wharf checks.	
		e. Control all exterior access points and principal interior access points to the seaport.	
		f. Have a sufficient number of guards to provide adequate security, 24 hours a day.	
		g. Be properly trained. Training is imperative for in-house or contracted security force personnel, all of which must receive adequate pre-work classroom training and be state certified (Class "D") license holders. Non-sworn security personnel working for a local law enforcement agency and assigned to the port do not require a Class "D" license. Training of security force personnel should address the following: • Patrol methods • Report writing, log and record keeping • ID of security problems and specific trouble areas	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		• Cargo handling and cargo documentation handling. • Federal security procedures (DOD 5225.22M , etc.),U.S. Customs, Immigration and Naturalization Service, and U.S. Coast Guard requirements • State procedures (including port authority) • Local police procedures, • Hazardous Materials Transport, Hazardous Materials Response • First aid • Use of force, Weapons use • Explosives, Nuclear, Biological, Chemical agent response • Terrorism response procedures • Labor unrest	
	6. Secure Information (INFOSEC)	a. Formal guidelines for computer security (INFOSEC) should be in place for each port and tenant activity.	
		b. Computerized information access must be password controlled, and should be restricted on a need-to-know basis, which would include dissemination of information no sooner than required.	
C. Cargo Security			
	1. Cargo Processing	a. Gate passes should be issued to truckers and other carriers to control and identify those vehicles authorized to pick up cargo.	
		b. Cargo should only be released to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified.	
		c. Personnel processing delivery orders should verify the identity of the trucker and trucking company before allowing entrance to or exit from restricted areas.	
	2. Storage of Loose Cargo	Cargo stored in open areas, and palletized or stacked cargo stored in warehouse facilities, must be properly stacked and placed within, away from, and parallel to, fences and walls, to ensure unimpeded views for security personnel.	
	3. High Value Cargo	a. High value commodities should be stored in cribs or security cages designed to resist forcible entry from all sides, and separate logs and procedures for the release and receipt of these commodities should be maintained.	
		b. High value merchandise in mounted containers must be placed in a secure holding area where it can be observed by management or security personnel, and separate logs and procedures for the release and receipt of these containers	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		should be maintained.	
		c. High value cargo containers requiring storage should be placed in a systematic manner such that their location is not readily apparent to would be criminals. Doors of high value containers should be stacked so that the doors of each container abut each other.	
	4. Equipment Control	Access and keys to cargo handling equipment such as yard mule tug-masters, trucks, or high loaders should be strictly controlled.	
		Cargo handling equipment should be kept in a secure and specified area when not in use.	
D. Cruise Operations Security			
	CG Regulations	a. Standards relevant to security of cruise ship operations are delineated by the USCG under 33 CFR Part 120 [Security of Passenger Vessels] and 33 CFR Part 128 [Security of Passenger Terminals]. Those with which port management should be most diligent in enforcing include the following:	
		b. Prevent or deter the introduction of prohibited weapons, incendiaries, or explosives into the terminal and its restricted areas and onto any passenger vessel moored at the terminal by persons, within personal articles or baggage, or in stowed baggage, cargo, or stores. 33 CFR 120.200 (a)(2) - …implement a [Vessel Security] program for that vessel that-- Prevents or deters the carriage aboard the vessel of any prohibited weapon, incendiary, or explosive, on or about any person or within his or her personal articles or baggage, and the carriage of any prohibited weapon, incendiary, or explosive, in stowed baggage, cargo, or stores; 33 CFR 128.300(a) (2) Deter the introduction of prohibited weapons, incendiaries, and explosives into the terminal and its restricted areas and onto any passenger vessel moored at the terminal; 33 CFR 120.300 (b)(2)- …[Vessel Security Plan must] Deter the introduction of prohibited weapons, incendiaries, or explosives aboard the vessel;	
		c. Maintaining a terminal security plan for each passenger terminal.	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		Sec. 128.300 What is required to be in a Terminal Security Plan? (a) If your passenger terminal is subject to this part, you must develop and maintain, in writing, for that terminal, an appropriate Terminal Security Plan that articulates the program required by Sec. 128.200.	
		d. Restricting the distribution, disclosure, and availability of information contained in terminal security plans to only those persons with an operational need to know. (6)(d) You must restrict the distribution, disclosure, and availability of information contained in the Terminal Security Plan to those persons with an operational need to know	
		e. Physical and operational security measures are coordinated between passenger terminals and passenger vessels whenever a vessel is moored at the terminal. 33 CFR 120.200 (a)(7) Provides for coordination with terminal security while in port. 33 CFR 128.200 (a)(7) Provides for coordination with vessel security while any passenger vessel subject to part 120 of this chapter is moored at the terminal.	
	Additional Port Management Responsibilities	a. In addition, port management will promote security of cruise operations by:	
		b. Providing SOPs for all security personnel (armed and unarmed) used at passenger terminals.	
		c. Providing and maintaining physical security such as barriers, alarms, and lighting in accordance with IMO circular 443.	
		d. Ensuring that vehicular access to cruise ships (while in port) is strictly enforced and that only authorized vendors are permitted access to cruise ships.	
		e. Providing communications between all security personnel involved with the security of passenger terminals and vessels	
		f. Establishing a system of identification and control for all personnel authorized access to the terminal.	
		g. Designating restricted areas for the embarking and disembarking of both passengers and baggage.	
		h. Ensuring that carriers provide timely, accurate and complete passenger and crew arrival and departure manifest information (in accordance with the Advanced	

Minimum Security Standards for Florida Seaports

(Note: Enhancements are regarded as part of the standard for Maximum Security Ports only)

Goal	Objective	Standard	Enhancements
		Passenger Information System) to the Immigration and Naturalization Service and the U.S. Customs.	
		i. Restricting access to passenger terminal facilities and cruise ships through a designated screening point that includes a metal detector and x-ray system for carry-on items (as a minimum).	
		j. In situations where the port does not provide terminal security guards, port management should ensure cruise terminal operators train security guards in accordance with the above provisions.	

FDLE
Side by Side

EXECUTIVE SUMMARY
FOR
FS 311.12 and 33 CFR Part 105
February 2004

BACKGROUND:
Passed into law in 2001, FS 311.12 has its genesis in counter-drug efforts in Florida's Public Ports. FS 311.12 mandates prescriptive security measures defined as "standards". In 2002 Congress passed the Maritime Transportation Security Act (MTSA), in response to International Maritime Organization requirements for seaport security, with supporting regulations published in the United States Code of Federal Regulations 33 CFR Part 101 and 105. FS 311.12 applies only to the public ports in Florida, while 33 CFR Parts 101 and 105 apply nationally to all seaports meeting the criteria described in Part 101. Facility as defined in 33 CFR Part 101/105 means any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or maintained by a public or private entity, including any contiguous or adjoining property under common ownership
or operation.

DISCUSSION: Florida seaports bound by FS 311.12 are also bound by the Federal regulations. Both FS 311.12, and the MTSA provide for seaport security, with FS 311.12 establishing specific action sets Florida Public Ports must comply with e.g., fencing, CCTV, lighting, access control procedures, and background screening. FS 311.12 is based in counter-drug, and loss prevention. FS 311.12 provided a security baseline, which has given Florida's Public Ports an advantage in development and implementation of the MTSA as defined in 33 CFR Part 105. Purpose of the MTSA is to prevent a Maritime Transportation Security Incident (TSI). This is accomplished through the prevention of loss of life, environmental damage, transportation system disruption, economic disruption to a particular area. Principles are balanced security and trade, understanding of port diversity, consistency, and performance based. The following bullets highlight the more salient requirements of both the FS 311.12 and the MTSA.

- **FS 311 .12** Applies only to FL Public Ports.
- **33 CFR Part 105** Applies to all U.S. waterway facility owners/operators meeting 101 criteria. MTSA aligns with ISPS Code/SOLAS and is defined through 33 CFR Part 101 and 105

- **FS 311.12** Prescriptive e.g. fencing, CCTV, locks, background screening, badging process
- **33 CFR Part 105** Performance based security, does not prescribe physical security standards e.g., fence, CCTV etc. Security must be commensurate with threat/ vulnerabilities and implemented through established MARSEC system.

- **FS 311.12** Requires constant manning of access points or use of electronic access control when access points are open.
- **33 CFR Part 105** Does not require manning of access points during MARSEC I, and only requires manning at higher MARSEC where screening is to occur.

Note: Although no specific language exist that requires manning in cargo security access points, MTSA uses language such as "performance based, and equivalent measures". USCG interprets this to mean that although they do not mandate a specific security measure, the facility security plan must provide for some type of performance based security that mitigates the established vulnerability.

- **FS 311.12** Does not establish job position or specific duties and knowledge for Facility Security Officers (FSO) positions
- **33 CFR Part 105** Establishes duties and knowledge for all FSOs. FSO must be identified to the USCG, and functions as the single POC on all security matters.

- **FS 311.12** Requires port management to establish Standing Security Committee comprised of key stake holders e.g., USCG, LE, BCBP, FDLE, Tenant Security Officers, meeting at least quarterly.
- **33 CFR Part 105** Requires USCG establish Area Maritime Security Committee comprised of key stake holders e.g., USCG, LE, BCBP, FDLE, Tenant Security Officers, meeting at least quarterly. All FSO are required to attend.

- **FS 311.12** Places responsibility on the public port for security and control of "High Value" cargo.
- **33 CFR Part 105** Places cargo security responsibility on owner/operators who are engaged in moving cargo.

- **FS 311.12** Established background screening requirements for personnel applying permanent port access credentials, as well as the Florida Uniformed Port Access Credential (FUPAC) in accordance, with criteria established by TSA for the Federal Transportation Workers Identification Cards "TWIC".
- **33 CFR Part 105** Defaults to the Transportation Workers Identification Cards "TWIC" which is in development.

- **FS 311.12** Requires risk assessment be conducted, but does not define standard or process.
- **33 CFR Part 105** Defines methodologies for risk assessment and vulnerability mitigation development by MARSEC.

- **FS 311.12** Requires Sworn LE on patrol.
- **33 CFR Part 105** Does not require sworn law enforcement on patrol.

Note: FS 311.12 mandate for sworn law enforcement on public ports was instrumental in maintaining FS 311.12 standards, as well as implementation of the MTSA

- **FS 311.12** Does not define Transportation Security Incident or procedures for reporting same.
- **33 CFR Part 105** Defines Transportation Security Incident and procedures for reporting same.

- **FS 311.12** Prescriptive requirements for certification, licensing, and employment of contract guards.
- **33 CFR Part 105** Defines training and knowledge requirements, with no certification or licensing established.

- **FS 311.12** Does not mandate specific requirements associated with drill, exercises, or security record keeping with the exception of maintaining a seaport security plan.
- **33 CFR Part 105** Requires training, quarterly drills, annual exercises and a requirement to maintain all security records for a period of two years.

- **FS 311.12** With the exception of access control, FS 311.12 defaults to USCG regulations for Cruise Terminal security
- **33 CFR Part 105** Provides prescriptive security measures for cruise terminal operation.

- **FS 311.12** Does not mandate or define requirements for interfacing with vessels.
- **33 CFR Part 105** Defines procedures and requirements for interfacing with vessels.

- **FS 311.12** Requires development of Critical Incident plans.
- **33 CFR Part 105** Requires development of Critical Incident plans.

• **FS 311.12** Makes no penalty, nor establishes a time line for obtaining compliance with **FS** 311.12.

• **33 CFR Part 105** Defines penalties, and deadlines (July 2004) for compliance. Penalties may include; (1) Restrictions on facility access; (2) Conditions on facility operations; (3) Suspension of facility operations; (4) Lesser administrative and corrective measures; or (5) Suspension or revocation of security plan approval, thereby making that facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the US. in accordance with 46 US.C.70103(c)(5). Civil penalty. As provided in 46 US.C. 70117, any person who does not comply with any other applicable requirement under this subchapter, including a Maritime Security Directive, shall be liable to the U.S. for a civil penalty of not more than $ 25,000 for each violation. Enforcement and administration of this provision will be in accordance with 33 CFR 1.07.

Side-by-Side Comparison of Federal and State Security Requirements

Issue	Federal Requirement	State Requirement
Statutory laws enacting seaport security standards and procedures	The Congress enacted the Maritime Transportation Security Act (MTSA) in 2002 – requiring federal seaport security standards and procedures. The U.S. Coast Guard developed rules and regulations pursuant to federal regulations act.	The Florida Legislature enacted section 311.12, F.S., in 2000, and formally adopted recommended standards contained in Camber Consulting Corporations report as state seaport security standards. No rule development requirements contained in section 311.12, F.S.
Flow of legitimate trade and travel	Maritime Transportation Security Act of 2002 (MTSA) provides Congressional findings and intent concerning "securing our borders without choking the flow of legitimate trade and travel."	No Legislative findings or intent in section 311.12, F.S., concerning flow of legitimate trade and travel.
Security Plans	MTSA requires public seaports, facilities on public seaports, and vessels transiting public seaports to have U.S. Coast Guard approved security plans. The U.S. Coast Guard has approved each individual Florida seaport security plan with respect to MTSA requirements. The U.S. Coast Guard has approved security plans for all cargo and cruise terminals on Florida's public seaports. Plans must be integrated with the respective U.S. Coast Guard Area Maritime Security Plan meeting MTSA requirements.	Section 311.12, F.S., requires only public seaports to have plans for entire seaport jurisdictional area. The FDLE has approved each individual Florida seaport security plan with respect to section 311.12, F.S., requirements. No similar requirement in section 311.12, F.S.
Risk Assessments	MTSA requires an updated 5-year risk assessment by public seaports, facility owner/operators. Risk assessment then used to update security plan every 5-years.	No similar requirement in section 311.12, F.S.

Issue	Federal Requirement	State Requirement
Security Personnel	MTSA requires trained security personnel to enforce security procedures and measures identified in security plans. No specific requirement on type of security personnel that can be used. Private sector cargo and cruise terminal operators on Florida's public seaports must have plans that provide and pay for additional security and access control measures at such terminals.	Section 311.12, F.S. is silent on specific requirement on type of security personnel. However, FDLE requires sworn law enforcement personnel at Florida's seaports. No similar requirement in section 311.12, F.S.
Access Control	MTSA requires access control at restricted (based on vulnerability/threat assessment) facilities. No similar requirement. No similar requirement.	Section 311.12, F.S. requires access control at restricted areas on Florida seaports. Section 311.12, F.S., requires criminal history background approvals for individuals working in restricted areas. Section 311.125, F.S., requires individuals permanently employed on or regularly accessing a seaport to use biometric uniform identification card to obtain access to restricted areas on Florida seaports.
Non-restricted/low-risk areas	No similar requirement: [MTSA requires identification of high-risk/vulnerable areas in risk assessment – security measures put in place for such areas.]	The FDLE interprets section 311.12, F.S. to require background checks on individuals employed in non-restricted/low-risk areas on seaports.
Public/private partnerships to enforce security zones.	MTSA authorizes identification and use of public/private partnerships that can be used in security zones to enforce security measures.	No similar authority in section 311.12, F.S. The FDLE has opined that port management must have control over tenant security and tenant security personnel.

Issue	Federal Requirement	State Requirement
Compliance Audits	All of Florida's public seaports are currently compliant with MTSA standards.	All of Florida's public seaports have been found to be substantially compliant with Florida's seaport security standards.
	The U.S. Coast Guard conducts unannounced audits and reviews throughout the year. The U.S. Coast Guard can shut down terminal operations, levy fines, and issue notice of compliance orders to seaports and private sector cargo and cruise terminal operators concerning failure to comply with federal security standards and procedures.	The FDLE conducts unannounced audits of public seaports every year. The result of this audit is delivered to the Governor and Legislature by December 31 of each year. The FDLE has no authority to fine, or shut down private sector cargo and cruise terminal operations.
	All entities with approved U.S. Coast Guard security plans are required to conduct an audit of the security plan's measures and procedures annually. Audits to be conducted by independent auditors pursuant to U.S. Coast Guard regulations – can be either governmental or private sector auditors.	No similar requirement in section 311.12, F.S.

Issue	Federal Requirement	State Requirement
Drug interdiction efforts	MTSA authorizes facilities and seaports to search vehicles and personnel entering designated restricted areas.	Section 311.12, F.S., provides no authority to seaport managers with respect to interdiction of drug and contraband. Section 311.12, F.S. provides no authority to seaport security personnel to detain, search, or hold suspect vehicles or personnel.
	U.S. Customs and Border Protections (CBP) primary federal entity with jurisdiction at U.S. seaports for interdiction of illegal drugs and contraband.	State and local law enforcement entities can participate with CBP for interdiction of illegal drugs and contraband at seaports.
	High Intensity Drug Trafficking Areas (HIDTAs) and Organized Crime Drug Enforcement Task Forces (OCDETFs) – federal, state and local law enforcement partnerships created by CBP around the country to interdict illegal drugs.	State and local law enforcement entities are partners in the HIDTAs in North Florida, Central Florida, and South Florida; and partners in the Florida/Caribbean OCDETF. Seaport managers are not law enforcement entities, and thus are not "partners" in any HIDTAs pr OCDETF.
Public/private partnerships to enforce security zones.	MTSA authorizes identification and use of public/private partnerships that can be used in security zones to enforce security measures.	No similar authority in section 311.12, F.S. The FDLE has opined that port management must have control over tenant security and tenant security personnel.

FISCAL YEAR SWORN LAW ENFORCEMENT COST FOR FLORIDA PUBLIC PORTS

February 15, 2006

FDLE

	FULL TIME LEO ON PORT	WRITTEN AGREEMENT	LEO SERVICES AT NO COST	GENERAL PORT SECURITY LEO COST	CRUISE TERMINAL SECURITY LEO COST	PUBLIC FACILITY LEO COST	SPECIAL EVENT LEO COST	LEO HOURLY RATE	PORT TOTAL LEO COST
PENSCOLA	NO	YES	NO CHARGE	$0	N/A	N/A	N/A	N/A	$0
PANAMA CITY	NO	YES	PARTIAL	$28,000	N/A	N/A	N/A	$16	$28,000
ST. PETERSBURG	NO	NO	NO CHARGE	$0	N/A	N/A	N/A	N/A	$0
MANATEE	NO	YES	NO CHARGE	$0	N/A	N/A	N/A	$27	$0
TAMPA	YES	YES	N/A	$1,592,000	$56,000	N/A	N/A	$28	$1,648,000
KEY WEST	YES					N/A	N/A		
MIAMI	YES	YES	N/A	$6,429,000	$2,352,000	N/A	PER EVENT	PER OFFICER	$8,781,000
EVERGLADES	YES	YES	PARTIAL	$7,989,492	$1,770,000	PER EVENT	PER EVENT	N/A	$9,759,492
PALM BEACH	YES	YES	N/A	$160,000	$190,000	N/A	$15,000	$25	$350,000
CANAVERAL	YES	YES	N/A	$1,361,000	$315,000	N/A	N/A	N/A	$1,676,000
JACKSONVILLE	YES	YES	N/A	$1,115,000	$137,000	N/A	N/A	N/A	$1,252,000
FERNANDINA	NO	YES	NO CHARGE	$0	N/A	N/A	N/A	N/A	$0
TOTAL				$18,674,492	$4,820,000				$23,494,492

1. Port of Tampa Cruise Terminal Cost does not include $166,000 for LEO traffic direction at street side terminal.
2. Port of Tampa public areas LEO patrol costs included in general port security costs.
3. Port of Miami public areas LEO patrol costs included in general port security costs.
4. Canaveral public areas LEO patrol costs included in general port security costs.
5. Special Event Costs identified not included in port totals.
6. BSO/Port Everglades reports some LEO services are provided without charge.
7. Panama City reports some routine patrol LEO services provided at no charge.

Florida Certified Port Protection Professional Basic Recruit Training Curriculum 218 Hours		
Unit Number	**Unit Title**	**Hours**
	Introduction	**15**
1	Overview of the Program	1
2	Criminal Justice System in Florida	3
3	Florida Constitutional Law – Search-Seizure-Detention	5
4	Criminal Justice Values and Ethics	2
5	Human Relations/Diversity	4
	Communications	**9**
6	Note Taking/Report Writing	4
7	Interviewing/Taking Statements	4
8	Use of Telecommunications	1
	Officer Safety Skills	**8**
9	Officer Safety and Survival Skills	8
	First Aid for Port Protection Professionals	**12**
10	Basic First Aid	4
11	CPR – IED	4
12	Response to Industrial Emergencies	4
	Security - Firearms	**28**
13	Florida Class G Security Officer Requirements	28
	Criminal Justice Defensive Tactics	**16**
14	Recognition of Criminal Justice Standards and Training Threat Matrix	
15	Restraint Devices	
16	Take Downs	
17	Pressure Points	
18	Counter Moves	
19	Escape Techniques	
20	Ground Control and Defensive Techniques	
21	Impact Weapons	
22	Defense Against Edged Weapons	
23	Handgun Retention/Disarming	
	Patrol	**16**
24	Patrolling Assigned Areas	
25	Detention and Custody	
26	Responding to Alarms	
27	Unknown Risk Vehicle Stops	
28	Unattended Vehicles	
	Law Enforcement Investigative Support	**4**
29	Preserving the Crime Scene	
	Hazardous Materials Response	16
30	Hazmat Response Training	
	Courtroom Procedure	**2**
31	Testifying in Court	1
32	Rules of Criminal Procedure	1
	Bombs and Weapons of Mass Destruction	**4**
	Bomb Threats	2
	Weapons of Mass Destruction	2
	Crowd Control	**4**
33	Demonstrators and Rioters	
34	Emergency Evacuations	

Unit Number	Unit Title	Hours
Familiarization with Port/Facility Security programs and regulations.		**14**
35	International Ship and Port Facility Security (ISPS) Code.	4
36	Maritime Transportation Security Act (MTSA)	4
37	Customs Trade Partnership Against Terrorism (C-TPAT)	2
38	Florida Seaport Security Standards (FS 311.12)	4
Familiarization with the roles of enforcement agencies with port security responsibilities		**8**
39	The United States Coast Guard (USCG)	
40	The Bureau of Customs and Border Protection (CBP)	
41	The Bureau of Immigrations and Customs Enforcement (ICE)	
42	The Federal Bureau of Investigations (FBI)	
43	The Florida Department of Law Enforcement (FDLE)	
44	Local Law Enforcement	
Security Threats and Patterns		**8**
45	Terrorism	
46	Illegal immigration	
47	Smuggling Alien/Narcotics/Other	
48	Other illegal activity Theft/Conspiracy/Racketeering	
Sensitive Security Information (SSI)		**2**
49	Handling of Security Sensitive Information (SSI)	
Security Vulnerability Assessment		**4**
50	Vulnerability Assessment	
51	Techniques used to circumvent security measures	
Maritime Security Organization		**4**
52	The Maritime Security Organization as outlined in the MTSA and ISPS Code.	
53	The Area Maritime Security Committee.	
54	The Regional Domestic Security Task Force	
Emergency Preparedness		**20**
55	National Incident Management System ICS 100/200, NMIS 700	
56	Security Drills and Exercises	
57	Weather Emergencies	
Threat Identification and Recognition		**8**
58	Methods of physical searches and non-intrusive inspections.	
59	Screening Procedures: Personnel/vehicles/cargo/stores	
60	Recognition of persons posing potential security risks	
61	Recognition and detection of weapons, dangerous substances and devices	
Security Equipment		**4**
62	Security equipment and systems limitations	
63	Operation of security equipment and systems	
64	Testing, calibration and maintenance of security equipment and systems	
Security Documentation		**4**
65	MTSA Required Reports	
66	Declaration of Security (DoS) agreement	
Seaport Security Credentialing		**8**
67	Florida Seaport Credentialing Requirements	
68	Federal Credentialing Programs	
69	Credentials for Foreign Mariners	

The POMTOC concept was conceived back in the early to mid 90s. The concept came about as a result of both Dodge and Lummus Island being completely developed in terms of cruise and container terminal yards. At that time, each individual stevedoring company had leased land from the Port Authority for their own container terminal. As happens today, carriers then often switched stevedores in response to marketplace competition, but since each stevedore had its own terminal area, the total terminal area required to operate far exceeded the capacity of the Port to keep up with the continued growth in demand.

In the face of this reality, the Port decided that the better approach would be to service this cargo in a single terminal, thereby reducing the overall space requirement while maintaining competition among the stevedores for vessel loading and unloading services.

The key drivers for the new terminal concept were:

A) The increase in volume was surpassing all previous growth projections.
B) The Port of Miami had/has a limited amount of acreage/land to handle containers (container terminal area)
C) The additional volumes could only be handled through efficiencies achieved by consolidation of all Independent stevedoring companies' container yard (terminal) operations;
D) The Port could only become more competitive through efficiencies of labor and equipment.

Due to the aforementioned points it was recommended that all existing independent stevedoring companies' container terminals had to consolidate into one single terminal operation or the Port would convert all existing container yards into a single County-owned and operated container terminal facility.

The independent stevedoring companies operating marine container yards and thus affected were namely 1) Continental Stevedoring & Terminals Inc. owned by Harrington & Company and Eller & Company; 2) Florida Stevedoring Inc ; 3) S.E.L. Maduro & Company, later purchased by I.T.O. Corp, and later P&O Ports of Fla; and 4) Oceanic Stevedoring Co., later purchased by P&O Ports.

Presently POMTOC membership is comprised of P&O Ports (50% founded in 1837); Florida Stevedoring (25% incorporated in 1972); and Continental Stevedoring (25% incorporated in 1985)

In order to avoid losing their marine container terminal business the Independent stevedoring companies agreed to consolidate and formed the Port of Miami Terminal Operating Co. LLC (POMTOC).

The formation of POMTOC served to unify the container terminal business of the Independents into one major CY, achieving better utilization of the limited land, and efficiencies of labor and equipment, including modern electronic terminal operating systems, to be able to reduce costs and effectively compete in an ever-changing Industry.

POMTOC has seen its total gate moves grow from 276,000 in the year 2000 to 373,000 in 2005, a 35% increase in 6 years. The Port of Miami has received $16.7m in revenue from POMTOC for land rental, container storage and office rental for the 6-year period, 2000-2005.

POMTOC has made capital investments in excess of $4.3 M for operating equipment, terminal operating systems and modular office units in the past three years and is committed to investing $12M in improvements over the next 5 years.

Port of Miami Overview

With record volumes of cargo and cruise passengers passing through the 518-acre island, the Port of Miami is one of America's busiest ports.

Cargo destined for more than 100 countries and 250 ports around the world flow through the Port of Miami. With that amount of destinations, the Port of Miami posted record numbers for the fourth year in a row. Last fiscal year, imports totaled some 5.7 million tons and exports were 3.7 million tons.

The Port of Miami continues to be the "Cruise Capital of the World," it saw a 3% increase in cruise passenger traffic, with more than 3.6 million vacationers taking to the high seas. In fact, there were 731 cruise dockings at the Port of Miami in 2005.

The Port of Miami is a major contributor to the economy of Miami-Dade County. It has an economic impact of $13 billion dollars and accounts for 93,000 jobs that are directly or indirectly related to port activities.

Overview of Security Enhancements

As the highly visible cruise capital of the world and cargo container gateway to Latin America, located just off-shore from the heart of downtown Miami, the Port of Miami has been working in conjunction with local, national and international security agencies to ensure it adequately responds to the new International Ship and Port Security (ISPS) Code requirements as well as the United States domestic Maritime Transportation Security Act which embarks a new, critical baseline of security.

Although implementation of these requirements may cause some disruption to the Port's day-to-day activities, these measures are required to ensure the safety of each and every person who does business with the Port. Our goal is

to minimize any disruption in the flow of commercial business through the Port, while meeting the new security requirements.

Security infrastructure improvements include the following projects:

(1) The installation of a CCTV Camera System throughout the Port
(2) Cargo and cruise terminal access control systems
(3) Cruise terminal door alarm system
(4) The redesign and construction of the main artery roadway that separates cruise and cargo vehicular traffic
(5) Identification Badge System

(1) CCTV Camera System
CCTV stands for Closed Circuit Television. It is a system in which the circuit is closed and all the elements are directly connected. It allows the Port to visually monitor high risk sensitive areas to protect against terrorist attacks, theft, fraud and to ensure employee safety. The system will eventually be housed at the Communication, Command and Control Center (C3).

(2) Cargo and cruise terminal access control systems
At the Port of Miami access control denotes anything that prevents or hinders entry, and thus decreases the opportunity for a security breach. Our state-of-the-art systems are managed by authorized personnel and serves as a deterrent to crime.

On the cruise side, in accordance with Federal regulations, the Port and cruise lines share the primary responsibility for shore-side and shipboard security of passengers. Passengers embarking on voyages at the Port of Miami must posses a boarding pass and have their baggage searched or passed through screening devices before boarding. Strict procedures are in place for passenger identification and visitor control.

On the cargo side, our integrated systems are equipped with gamma ray technology to scan incoming containers. Additionally, all persons entering the restricted cargo area undergo an extensive background check and are required to be properly credentialed.

(3) Cruise terminal door alarm system
At the Port of Miami a state of the art door alarm system is in place and is programmed to siren at the first sign of intrusion.

(4) Redesign and construction of the main artery roadway
The newly redesigned roadway system has been constructed, separating cruise and cargo traffic into two distinct districts. This results in increased safety of cruise passengers by preventing entry into restricted access areas beyond the cargo security gateway.

(5) Identification Badge System
At the Port of Miami all persons requesting ID cards are subject to a comprehensive criminal background check that includes the submission of fingerprints and a status check on their driver's licenses. Any person providing false information on their ID application shall be denied an ID card and will face possible prosecution.

Port of Miami's Security Challenge - Funding

The Port of Miami is continuously working to secure funding from state and federal sources for security operations. In the aftermath of the tragic events of September 11, 2001, the Port has continued to increase its annual operating security-related operating costs to almost $17 million for fiscal 2005, or more than three times as much as fiscal 2001's $4.1 million budget. As of September 2005, total security capital projects exceed $64 million.

Thus, one of the biggest challenges the Port faces is funding security related costs.

To achieve security infrastructure needs for funding assistance, the Port of Miami has aggressively applied for security grants from State and Federal programs. To date, the Port has received in excess of $19.4 million in Federal funds and has also been successful in getting more than $9.4 million in State Commerce grants funds re-allocated for security projects. These are among the highest of such awards across the nation.

DP World - Background

General

- DP World is a global ports and terminal operator that is internationally recognized for its quality, service and customer satisfaction. Since 2001 it has embarked on a growth strategy that will catapult it to top-three status. With the intended purchase of P&O it will have operations in 50 ports, 30 countries and six continents.

- DP World retain a truly independent "common user terminal" status which ensures efficiency and dedication to customer needs. DP World bring a unique suite of operational expertise: container terminals, general cargo terminals, free trade zones (including the world's largest), customs, and logistics centers.

- Dubai is not a large country and thus management of its global commercial ventures requires an international diverse team. The renowned management team is truly multinational including citizens of the United States, Australia, United Kingdom, India and the Netherlands. For example the Chief Operating Officer, General Counsel and Head of Business Development are all United States citizens. This will be even more the case following the acquisition of P&O.

- DP World is a multinational company based on Dubai, which sits astride the shipping lanes from Europe and Africa to Asia.

- Jebel Ali in Dubai was the original cornerstone facility, the largest container port between Rotterdam and Singapore, and the tenth largest global terminal overall. DP World sprung from this base, which is growing to become a massive transhipment center and free zone that is expanding to 130 kilometers, including a six runway airport.

- Before the intended purchase of P&O, DP World already had a global reach of 22 container terminals, four free zones and three logistics centres. That will now expand to 50 operations in 30 countries.

- DP World is commercially focused, an enterprise of the Dubai government. It is part of a group of highly successful commercial ventures that take advantage of commerce to fuel the economy. These include world-renown Emirates Airlines and landmark property developments both internationally and locally.

- DP World's purchase of P&O is largely funded through a $6.5 billion syndicated debt deal underwritten by Deutsche Bank and Barclay Bank which is currently being syndicated on the international banks market.

- DP World's expansion started hitting stride with the $1.14 billion purchase of US terminal and shipping concern CSX-WT in early 2005. The intended P&O takeover is part of an expansion policy designed to make DP World a global heavyweight on par with Hong Kong's Hutchison, Singapore's PSA and Denmark's Maersk.

P&O Ports North America Inc, and DP World - Security

General:

- Globally DP World has received all the necessary regulatory approvals regarding the intended acquisition of P&O.

  In addition to the United States, P&O Ports operate in Argentina, Australia, Belgium, Canada, China, France, India, Indonesia, Mozambique, New Zealand, Pakistan, Papua New Guinea, Philippines, Russia, South Africa, Sri Lanka, Thailand and the United Kingdom.

  DP World existing operations are located in Australia, China, Dominican Republic, Germany, Hong Kong, India, Romania, South Korea, UAE and Venezuala.

- In the United States the intended purchase has been approved by the Committee on Foreign Investment in the United States (CFIUS). CFIUS implements an Exon-Florio provision to provide a mechanism to review and, if the President finds necessary, to restrict Foreign Direct Investment that threatens the national security. The CFIUS comprises 12 government departments and agencies, these being :-

  Department of Defense
  Department of Homeland Security
  Customs and Border Protection
  United States Coastguard
  Department of Transportation
  Office of the United States Trade Representative
  Office of Management and Budget
  Office of Science and Technology Policy
  Department of Treasury
  Department of Justice
  Department of Commerce
  Department of State

  Unanimous approval was granted.

- Security at US ports is directly overseen by the United States Coastguard and by Customs and Border Protection. P&O Ports North America Inc, is a long standing member of the Customs-Trade Partnership against Terrorism (C-TPAT). P&O Ports North America Inc is committed to maintaining and enhancing their leading role.
- P&O Ports North America Inc, will continue to operate after the intended acquisition as the North American operating arm of the company. P&O Ports North America Inc will directly report to P&O SN Co in London. The management of P&O Ports North America Inc will remain in place unchanged.
- P&O Ports North America Inc, lease and operate terminals, they do not own ports. Through concession and operating agreements P&O Ports North America Inc provide services to Ports, Shipping Lines and Cargo Owners.

- DP World and P&O Ports North America Inc jointly filed a notification of the acquisition to the CFIUS on December 15, 2005, consistent with Section 721 of the Defense Production Act of 1950, as amended, and U.S Department of the Treasury Regulations at 31 CFR Part 800.

- The CFIUS reviewed the notification and concluded, by letter dated January 17, 2006, that the acquisition did not raise issues of U.S. national security sufficient to warrant an investigation.

- DP World explained its commercial position as the seventh largest global ports operator and explained its desire to acquire P&O for commercial reasons, based on its analysis of its business needs, including the complementary operations of the two companies.

- P&O Ports North America Inc and DP World have expressly committed to maintain and, as appropriate, expand all existing security arrangements and commitments of P&O Ports North America Inc. Moreover, even though it has not previously held concessions to US operations, DP World already participate in US security programs in their global operations including the Customs Trade Partnership against Terrorism and the Container Security Initiative which includes US Customs and Border Patrol offices in Dubai.

- The Governments of the United Kingdom and Australia also reviewed in specific detail the P&O acquisition by DP World and raised no objections to the transaction.

END

Dubai Ports World Intended Purchase of P&O Fact Sheet

General:

- With the acquisition of P&O, DP World will jump from seventh to third in global port operator rankings, with 51 terminals in 30 countries on five continents. Our capacity will be 50 million TEU.

- This was a commercially driven and completely transparent takeover of a UK listed company underwritten by Barclays and Deutsche Bank. The purchase has been approved by P&O shareholders and the two companies are in the process of integrating.

- The ports industry is an economic cornerstone for Dubai. DP World believes that the offer for P&O has compelling strategic logic and creates significant opportunities for companies, customers and employees going forward. In particular, the combination will:

  - Enhance DP World's position as a top 3 global ports operator
  - Address the needs of a consolidating liner shipping customer base
  - Offer an unparalleled complementary geographical fit
  - Provide significant additional capacity in key markets
  - Bring together some of the most experienced people in the industry
  - Provide a strong company willing to invest in much needed infrastructure to support the growth of global trade.
  - Provide complete continuity of management within P&O Ports North America Inc and further opportunities for growth in the Americas market.

- Currently, DP World operates 22 container terminals, 4 free zones and 3 logistics centers. DP World have operational offices in 15 countries. DP World current capacity is 20 million TEUs. DP World also has a number of very large port development projects underway such as Pusan in Korea, Qingdao in China and Cochin in India. The key numbers:

	Metric	DPWorld	P&O	Combination
Number of terminals	No.	22	29	51
Number of countries	No.	15	18	30
Current gross capacity	TEUm	20	30	50
Global ranking	No.	7	4	3

- The terms: 520 p in cash for each outstanding P&O deferred share, representing a premium of 71.3% to the closing price of 303.5 p for each unit of deferred stock on 27 October 2005 (being the last day prior to speculation regarding a possible offer for P&O). Equity value of bid: £3.9 billion.

- The bid has been financed entirely through conventional funding. As required by the UK Takeovers Code DP World have committed financing in place. DP World only ever enters into deals that make commercial sense. The bulk of the financing is from a $6.5 billion syndicated debt deal underwritten by Deutsche Bank and Barclays which is currently being syndicated on the international banks market..

- The combined businesses present a number of attractive growth opportunities. It builds on both DP World's and P&O's established global networks and reputation for excellence to better serve our combined customers.

- DP World have passed regulatory requirements in several countries, including Australia and the United Kingdom which had no security concerns about the change in ownership.

END